UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,459	08/20/2003	Manish Rathi	2717P100	8009

8791 7590 03/20/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/645,459	RATHI ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/18/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18,19 and 21-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18,19 and 21-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/18/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on December 18, 2007.

2. Claims 1-16, 18-19 and 21-25 have been examined and are pending.

Response to Arguments

3. Applicant's arguments filed on December 18, 2007 have been fully considered but they are not persuasive.

The applicant argues that "Causing a switch "to **block network traffic**" in response to a "**failed authentication**" is not the same as "**sending an unblock port command** .when the authentication routine results in a **positive authentication response**. Indeed, Droms provides functionality that is essentially opposite of the embodiment Applicants recite in claim 1, and thus does not disclose the limitation "sending an **unblock port command** ... when the authentication routine results in a **positive authentication response**."

The examiner disagrees with the applicant's analysis because Droms teaches "sending an unblock port command" recited in the following section with emphasis added in bold and italics.

(Column 2: lines 20-37)

The information sent by the supplicant might be stored persistently on the host being connected; or the information might be received from a human user of the host, such as *in*

response to prompts for user name and password; or some combination of stored and user-supplied information may be used. The *intermediate device runs an authenticator process*, hereinafter called the *authenticator*. The authenticator sends a request to an authorization, authentication and accounting ("AAA") system based on the information from the supplicant. .. The AAA system returns a ***response indicating whether the connection should succeed or fail***. ***If the response indicates the connection fails,*** *the* ***intermediate device does not forward data*** communicated to the physical port from the host. ***If the response indicates the connection succeeds***, the ***intermediate device does forward data communicated to the physical port from the host***..... After ***obtaining access through the physical port*** and receiving a configuration, a client on the user's host may request services from servers on the network using IP.

(Column 14: lines 10-25)

In step 440, a test is performed to determine whether the user is authorized to connect to the network. For example, it is determined whether *the response from the authentication and authorization server indicates that* ***the user is both authentic and authorized to connect*** *to the local network*. If not, *control passes to step 442* ***to block network traffic through that port*** *and to send a message to the host that network access is rejected*. For example, ***the port is not enabled,*** and an IEEE 802.1x message that ***negates acknowledgement*** (an IEEE 802.1x "NAK" message) is sent to the newly connected host 122. If the test of step 440 determines ***that the user is authorized to connect to the network***, **control passes** to step 444. In step 444, ***the physical port is enabled so that network traffic is passed***. According to the IEEE 802.1x standard, an acknowledgement message is sent to the newly connected host 122.

Therefore, the applicant's argument is not persuasive to overcome Renda in view of Droms to place independent claim 1 in condition for allowance. An independent claim 18 is not placed in condition for allowance for the same reason. Dependent claims 2-16, 19 and 21-25 are also not placed in condition for allowanced based on their dependency.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-16, 18-19 and 21-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Renda et al. (hereinafter referred to as Renda, US. Pat. No.: 7, 127, 524) in view of Droms et al. (hereinafter referred to as Droms, US Pat. No.: 7, 143, 435).

As per claim 1:

Renda discloses a method comprising:

Intercepting a request for a web page from a user device (column 3: lines 60-67; column 9: lines 55-67; figure 2A, 2B);

directing the user device with a network login page for authentication (figure 8A: 832,822B; column 24: lines 50-60; column 25: lines 43-61; column 27: lines 35-50);

executing an authentication routine to authenticate the user device based on input received at the network login page (column 23: lines 65-67; column 24: lines 1-12; column 25: lines 16-26); and

allowing the user device to access the network when the blocked port is unblocked (column 8: lines 1-35).

Renda does not explicitly disclose the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled to the forwarding device and sending an unblocked port command to unblock the blocked port when the authentication routing results in a positive authentication response for the user device. Droms, in analogous art, however discloses the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled to the forwarding device and sending an unblocked port command to unblock the blocked port when the authentication routing results in a positive authentication response for the user device (Column 2: lines 20-37; Column 14: lines 10-25; Column 9: lines 45-65; the authenticator 105 sends a request 224 to the RADIUS server 135 according to IEEE 802.1x. The request 224 includes at least some of the information about the host and user received in the request 222. The RADIUS server then determines whether the user is authentic based on the user information and, if so, whether the authentic user is authorized to connect to the local network. If the user is not authentic or not authorized to connect, a response is sent indicating that authentication fails, according to IEEE 802.1x. In response to a failed authentication, the authenticator causes the switch to block network traffic with the host through the physical port 104b).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Renda et al. to include the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled to the forwarding device and sending an unblocked port command to unblock the blocked port when the authentication routing results in a positive authentication response for the user device. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a protocol for controlling access to LAN resources based on a physical port, and with a configuration server, and with an authentication and authorization server as suggested as suggested by Droms in (column 6: lines 25-35).

As per claim 2:

Renda discloses a method, wherein intercepting a request from the user device comprises intercepting a Hypertext Transfer Protocol (HTTP) request from the user device (column 12: lines 17-33; column 23: lines 34-65; column 18: lines 1-20).

As per claim 3:

Renda discloses a method, comprising receiving a Domain Name Service (DNS) request to translate a domain name specified in the HTTP request into an Internet Protocol (IP) address (column 4: lines 1-50; column 14: lines 45-55; column 12: lines 56-65).

As per claim 4:

Renda discloses a method, comprising proxying the DNS request to a DNS server (column 7: lines 45-60).

As per claim 5:

Renda discloses a method, comprising receiving a response from the DNS server with a DNS-resolved IP address (column 7: lines 45-60; column 43: lines 35-55).

As per claim 6:

Renda discloses a method, comprising sending the DNS-resolved IP address to the user device (column 7: lines 45-60; column 43: lines 35-55).

As per claim 7:

Renda discloses a method, comprising intercepting a request from the user device directed to the DNS-resolved IP address (column 7: lines 45-60; column 43: lines 35-55).

As per claim 8:

Renda discloses a method, wherein directing the user device to a network login page for authentication comprises responding to the user device with a redirect to a Uniform Resource Locator (URL) address for the network login page (column 12: lines 17-33; column 23: lines 34-65; column 18: lines 1-20).

As per claim 9:

Renda discloses a method, comprising receiving a DNS request from the user device to translate a domain name for the network login page into an IP address (column 4: lines 1-50; column 14: lines 45-55; column 12: lines 56-65).

As per claim 10:

Renda discloses a method, comprising responding to the user device with the IP address of the packet forwarding device (figure 8A: 832, 822B; column 24: lines 50-60; column 25: lines 43-61; column 27: lines 35-50).

As per claim 11:

Renda discloses a method, comprising receiving from the user device a request to the 1P address of the packet forwarding device (column 3: lines 60-67; column 9: lines 55-67; figure 2A, 2B).

As per claim 12:

Renda discloses a method, comprising responding to the user device with the network login page (column 23: lines 65-67; column 24: lines 1-12; column 25: lines 16-26).

As per claim 13:

Renda discloses a method, comprising receiving an authentication request from the user device via the network login page, the authentication request comprising user identification user identification data (column 23: lines 65-67; column 24: lines 1-12; column 25: lines 16-26).

As per claim 14:

Renda discloses a method, wherein executing the authentication routine to authenticate the user device based on input received at the network login page comprises parsing the authentication request and forwarding the authentication request to an authentication server (column 26: lines 5-40).

As per claim 15:

Renda discloses a method, wherein parsing the authentication request and forwarding the authentication request to the authentication server comprises creating a packet with the user identification data in accordance with the RADIUS communications protocol and forwarding 4 the RADIUS packet to a RADIUS server (column 26: lines 5-40; column 24: lines 50-67).

As per claim 16:

Renda discloses a method, comprising receiving a response from the RADIUS server to indicate whether the user identification data is authentic (column 26: lines 5-40; column 24: lines 50-67).

As per claim 17:

Renda discloses a method, wherein allowing the user to access the network when the user is authenticated comprises unblocking the blocked port of the packet forwarding device to allow the user to access the network when the user is authenticated (column 8: lines 1-35).

As per claim 18:

Renda discloses an apparatus comprising:

a packet forwarding device coupled with a network, (column 3: lines 60-67; column 9: lines 55-67; figure 2A, 2B; figure 8A: 832, 822B; column 24: lines 50-60; column 25: lines 43-61; column 27: lines 35-50); and

an authenticator discovery controller coupled with the packet forwarding device, the authenticator discovery controller to intercept a request for a web page from the user device direct the user device to a network login page for authentication, the authentication controller (column 23: lines 65-67; column 24: lines 1-12; column 25: lines 16-26; column 8: lines 1-35).

executing an authentication routine to authenticate the user device based on input received at the network login page (column 23: lines 65-67; column 24: lines 1-12; column 25: lines 16-26; column 8: lines 1-35), and

Send an unblocked port command to unblock the blocked port, when the authentication routine result in a positive authentication response for the user device.

Renda does not explicitly disclose the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled to the forwarding device and sending an unblocked port command to unblock the blocked port. Droms, in analogous art, however discloses the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled

to the forwarding device and sending an unblocked port command to unblock the blocked port (Column 2: lines 20-37; Column 14: lines 10-25; Column 9: lines 45-65; the authenticator 105 sends a request 224 to the RADIUS server 135 according to IEEE 802.1x. The request 224 includes at least some of the information about the host and user received in the request 222. The RADIUS server then determines whether the user is authentic based on the user information and, if so, whether the authentic user is authorized to connect to the local network. If the user is not authentic or not authorized to connect, a response is sent indicating that authentication fails, according to IEEE 802.1x. In response to a failed authentication, the authenticator causes the switch to block network traffic with the host through the physical port 104b). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Renda et al. to include the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user from accessing a network coupled to the forwarding device and sending an unblocked port command to unblock the blocked port. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a protocol for controlling access to LAN resources based on a physical port, and with a configuration server, and with an authentication and authorization server as suggested as suggested by Droms in (column 6: lines 25-35).

As per claim 19:

Renda discloses an apparatus, comprising when the authenticating routine to authenticate the user device based on input received at the network login page comprises sending the input

received to network login controller coupled with the packet forwarding device to authenticate the user device based on input received and send the positive authentication response to the authenticator discovery controller when the user device is successfully authenticated (figure 2B: 274, 292).

As per claim 21:

Renda discloses an apparatus, wherein the unblocked port command to unblock the blocked port originates at the network login controller (column 8: lines 1-35).

As per claim 22:

Renda discloses an apparatus, wherein the authenticator discovery controller to further receive a Domain Name Service (DNS) request from the user device and to proxy the DNS request to a DNS server to translate a domain name into an Internet Protocol (IP) address (column 4: lines 1-50; column 14: lines 45-55; column 12: lines 56-65).

As per claim 23:

Renda discloses an apparatus, wherein the packet forwarding device is a switch (column 16: lines 25-40).

As per claim 24:

Droms discloses a method, wherein the blocked port comprises a default state, the default state characterized as operating in a non-forwarding, un-authorized, and blocked functionality mode (Column 2: lines 20-37; Column 14: lines 10-25).

As per claim 25:

Droms discloses a method, wherein the blocked port returns to the default state after one or more events including:

a pre-determined period of inactivity by the authenticated user device is exceeded; a reset signal is received from a network login controller; an administrator forces the blocked port back to its default state; a network connection associated with the authenticated user device is disconnected; and a user of the authenticated user device logs off of the authenticated user device (Column 9: lines 45-65).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137